

## Cyber Security is our mission

### events

#### Symposium on Digital Behaviour Intervention for Cyber Security

Location: Liverpool, UK

Date: March 4-6, 2018

<https://www.sspedi.co.uk/aisb2018>

Symposium on Digital Behaviour Intervention for Cyber Security (AISB18-CyberSecurity) is categorized in our directory with the following tags: Liverpool Events / UK Cybersecurity Conferences.

This symposium focuses on how digital technology can motivate and influence people to behave more cyber-securely. It will bring together researchers, designers, developers and cyber-security experts interested in computers designed to change cyber-security attitudes and behaviours. The symposium will cover a wide range of topics on persuasion, from behaviour intervention methods to persuasive argumentation and persuasive user interfaces.

#### Cyber-Crime Conference 2018

Location: Rome, Italy

Date: April 18, 2018

[https://www.ictsecuritymagazine.com/event/cyber\\_crime\\_conference\\_2018/presentation](https://www.ictsecuritymagazine.com/event/cyber_crime_conference_2018/presentation)

This 9th edition will open with a Round Table dedicated to "Machine Learning Systems, Blockchain, IoT and Big Data in the hands of Cyber Criminals". At Conference will be discussed the most topical issues: from the GDPR and its implications in terms of Privacy and Cyber Hygiene to the new, complex scenarios outlined by the Cyber Warfare and the Cyber Weapons; from the challenges of Cyber Defense in the IoT Era to the techniques of Digital and Mobile Forensic, Deanonymization and Blockchain without neglecting their innumerable legal, technological and financial implications.

#### EuroCyber: Are you business-ready for GDPR?

Location: Rome, Italy

Date: May 9-10, 2018

<https://skytopstrategies.com/eurocyber-2018-italy/>

GDPR Implementation and its Impact on Multinational Company Compliance and Cybersecurity. The EU General Data Protection Regulation (GDPR) is set to take effect May 25, 2018 and with it comes a host of changes to personal data protection laws. This full day discussion will focus on how companies are efficiently implementing and complying with GDPR and understanding the consequences of non-compliance, as well as discussing how companies based outside of the EU who do business within the EU are affected by GDPR.

#### ENISA Industry Event - Certification, IoT and collaboration

Location: Bruxelles, Belgium

Date: April 24, 2018

<https://www.enisa.europa.eu/events/enisa-industry-event-2018/it-security-industry-collaboration-event>

ENISA's Industry event will provide the participants with an overview of the proposed EU Certification framework and how this relates to the EU cyber security industry, whilst focusing on the proposed outline and scope of the proposed legislation. The discussion will continue with key topics such as the Internet of Things, in relation to the Industry 4.0 concept and its effect on end users. With this event ENISA aims to increase the interconnectivity among the ENISA Industry Event Members.

### news

**Gits club GitHub code tub with record-breaking 1.35Tbps DDoS drub**  
[https://www.theregister.co.uk/2018/03/01/github\\_ddos\\_biggest\\_ever/](https://www.theregister.co.uk/2018/03/01/github_ddos_biggest_ever/)

What's purported to be the world's largest distributed denial of service attack to date – measuring 1.35Tbps – knocked GitHub offline for a few minutes yesterday.

The massive tsunami hit at 1721 UTC. During the assault, the popular code sharing website's admins noticed thousands of systems and devices slamming GitHub's web servers. Inbound network traffic peaked at 1.35Tbps, or 126.9 million packets per second, [...]

**New vulnerability in Exim software allows hackers to gain control of your mail server**

<https://threatpost.com/venerable-unicode-technique-used-to-deliver-cryptomining-malware-through-telegram/129929https://www.techrepublic.com/article/cve-2018-6789-vulnerability-in-exim-mail-server-software-allows-remote-code-execution/>

A critical vulnerability has been discovered in Exim, a widely deployed mail transfer agent. With a specifically crafted mail message, an attacker can exploit an off-by-one buffer overflow due to mishandling of base64 authentication. Because of the nature of the vulnerability, particularly relating to how SMTP transactions are conducted, it is possible for attackers to exploit remotely without authentication.[...]

**Big Data And AI For Predicting Human Behaviour**

<https://www.cybersecurityintelligence.com/blog/big-data-and-ai-for-predicting-human-behaviour-3222.html>

Data has led to numerous innovations and discoveries. At the same time, it has also pioneered several technologies that depend upon artificial intelligence (AI). There is hardly any industry that is not trying to inculcate artificial intelligence and use big data for better analysis of [...]



# *Happy Easter*

